VPN auf Pi-Star einrichten

hier wird beschrieben, wie ein Wireguard Client eingerichtet wird.

System vorbereiten

Aktualisieren

```
sudo apt update
sudo apt upgrade
```

falls es ReadOnly mounts gibt, diese ReadWrite machen

Das folgende trifft u.U, nur auf pi-star zu, nicht auf WPSD, jedenfalls habe ich bei WPSD keine ro Partition gesehen. Das kann man prüfen mit: findmnt -o TARGET,FSTYPE,OPTIONS

Bevor Änderungen gemacht werden, muss das System ReadWrite geschaltet werden:

```
sudo mount -o remount,rw /dev/mmcblk0p2  /
```

(nach dem nächsten booten schaltet er automatisch wieder auf ReadOnly)

die Linux firewall (iptables) ist aktiviert

Es müssen die von Wireguard benutzten Ports freigegeben werden, das ist standardmäßig Port 51820.

Um Erweiterungen der Firewall permanent hinzuzufügen, gibt man diese in die Datei /root/ipv4.fw ein:

```
iptables -A INPUT -p udp --dport 51820 -j ACCEPT
iptables -A OUTPUT -p udp --dport 51820 -j ACCEPT
```

danach die Eintragungen ausführen:

```
sudo pistar-firewall
```

Prüfen ob die Firewall UDP auf dem Port durchlässt

dieses Kommando lauscht auf eingehende Nachrichten:

```
socat -u UDP-LISTEN:51820,reuseaddr,fork STDOUT
```

auf dem Rechner wo der Wireguard Server läuft führt man aus:

```
echo "Test message" | nc -u -w 1 <IP des Client> 51820
```

Wireguard installieren

```
sudo apt install wireguard
```

Wireguard konfigurieren

erzeuge die Schlüssel für den Client

```
(umask 077 && wg genkey > wg-private.key)
wg pubkey < wg-private.key > wg-public.key
```

erstelle die Client Konfigurationsdatei:

```
sudo nano /etc/wireguard/wg0.conf
```

und schreibe hinein:

```
# define the local WireGuard interface (client)
[Interface]

# contents of file wg-private.key that was recently created
PrivateKey = MD......OSGVw=

# The IP address of this client in the WireGuard network
Address = 10.0.2.2/32

# The port on which the WireGuard client will listen (optional if the client
is not behind NAT)
ListenPort = 51820

# define the remote WireGuard interface (server)
[Peer]

# contents of wg-public.key on the WireGuard server
PublicKey = dhVt......4rjHzA=

# AllowedIPs defines which IP addresses are routed through the VPN.
# To route only specific traffic, adjust as needed. To route all traffic
through the VPN, use 0.0.0.0/0.
AllowedIPs = 10.0.0.0/16

# public IP address and port of the WireGuard server
Endpoint = <IP or URL of the wireguard server>:51820

# Keepalive interval, useful if either side is behind NAT (optional)
```

```
PersistentKeepalive = 25
```

Wireguard nach dem Booten automatisch starten

```
sudo systemctl enable wg-quick@wg0
```

Wireguard manuell starten

```
sudo systemctl start wg-quick@wg0
```

das Interface starten/stoppen

nur optional, obiges systemctl-Kommando reicht

```
sudo wg-quick up wg0
sudo wg-quick down wg0
```